HARMONY IoT
BY ORCHESTRA GROUP

Harmony IoT: Wireless Airspace Security for Hospitals

Hospitals are frequent targets of cyberattack. Data breaches, ransomware and threats to patient safety are on the rise, but hospital CIOs must manage security with tight budgets and lean staffing. Adding to this challenge is one simple truth – lives are at stake.

THE WIRELESS AIRSPACE SECURITY GAP

Because hospitals are open to the public, attackers have unchecked access to the airspace both from within hospital buildings as well as from the surrounding areas. Attackers can easily find and compromise wirelessly connected devices - tablets, IoT and IoMT that are used everywhere in hospitals. They can use that access to steal patient data, install ransomware, and even interfere with medication delivery. Current security tools such as traditional NAC (network access control) systems and MDM (mobile device management) systems lack visibility into many devices in the hospital environment and do not monitor activity in the airspace. In short, traditional NAC and MDM solutions do not prevent the hospital airspace from being used as an attack vector.

HARMONY IoT – SECURING THE HOSPITAL AIRSPACE

Harmony IoT is a complete airspace security solution that delivers visibility, continuous monitoring, and real time attack mitigation. Its policy engine makes it easy for IT staff to set and enforce airspace security policies, and it provides automated compliance reporting tailored for wireless security standards. Finally, Harmony IoT is non-invasive: It is an **out-of-band solution** that requires no changes to the network. That means rapid time to implementation and low TCO.

- Simple Integration
- Zero Touch
- Self Managed
- Self Healing

Harmony IoT Cloud Service

- Various Feeds
- Harmony IoT Dashboard
- Harmony IoT Protectors

HOW IT WORKS

Harmony IoT is a cloud managed solution comprising small sensors (Smart Protectors) that monitor the hospital airspace and send data to the Harmony IoT cloud. The sensors use information from the data link layer to secure the airspace. They do not collect any sensitive/confidential information. Each Smart Protector processes large amounts of data locally and sends a much smaller volume of meta-data to the Harmony IoT cloud for analysis and reporting.

The heart of Harmony IoT is an AI/big data system that continuously learns from all Smart Protector deployments. Harmony IoT identifies what is normal/suspicious in terms of device type as well as what is normal/abnormal behavior in the context of each customer environment. Unlike signature-based systems which are easy to defeat, Harmony IoT identifies and mitigates attacks even as attackers evolve their methods to escape detection by traditional WIPS (wireless intrusion prevention systems).

FEATURES AND BENEFITS

Full Visibility
Detects what devices (device type, manufacturer, model) are present in the airspace - regardless of what network they belong to, or even if they are attached to a network.

Continuous Monitoring
Records when devices appear and disappear from the airspace, attempts to connect to a network (SSID), attempts to establish an access point or network, suspicious activity, and anomaly detection.

Policy Management
Set and enforce security standards such as Wi-Fi encryption and authentication standards, what is allowed by location, device type, time of day/day of week. Device white and blacklisting.

Restricted Area Policy
Only known, trusted devices are allowed in designated areas such ERs and ORs.

Alerts and Mitigation
Mitigate attacks in real time. Mitigations can be automated or under operator control. Mitigations are immediate and target only the offending device.

Location Sensing
Harmony IoT reports on the location of every device operating in the airspace. This makes it easy to pinpoint the location of any offending device, drastically reducing the time to fully mitigate.

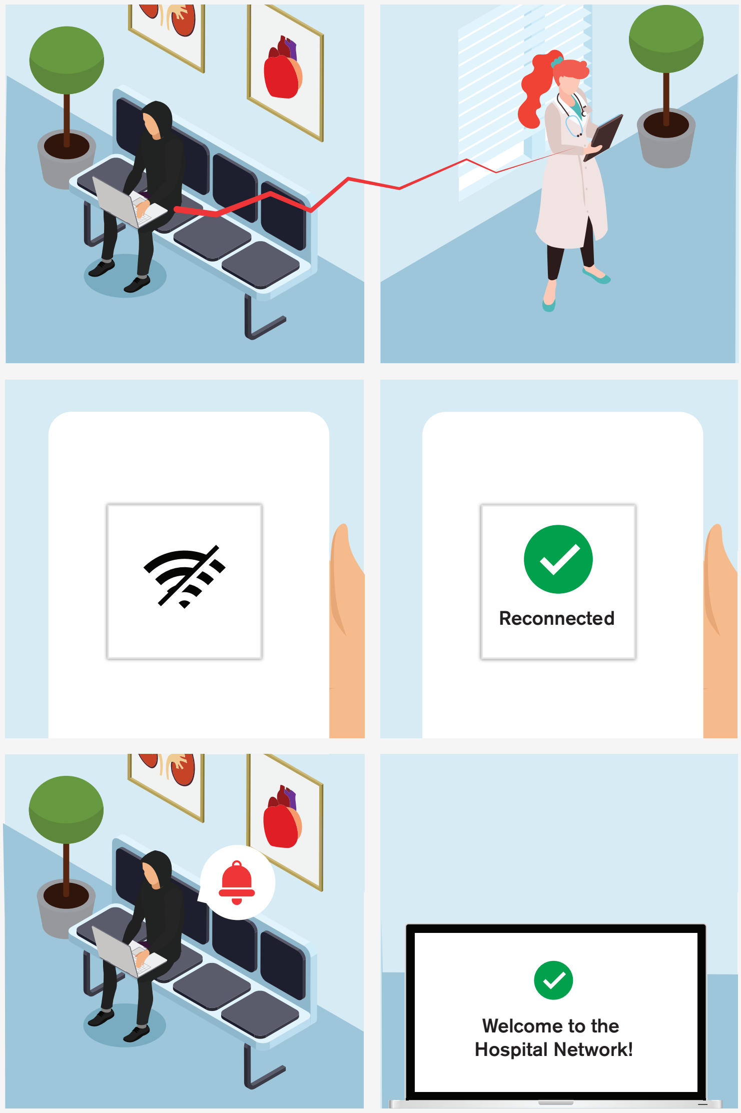
Compliance Reporting
Harmony IoT generates compliance reports that expose issues needing attention and provide assurance that compliance policies and security mandates for the airspace are being met.

Out of Band
Harmony IoT passively monitors activity in the airspace and needs no connection or resources from the host network. It requires no internal resources (IP addresses, DNS, software updates, etc.) from IT operations staff.

CASE STUDY
HARMONY IoT PROTECTS MEDICAL EQUIPMENT AT MULTIPLE CLINICS

A large, distributed health care provider in Israel with many branch locations needed to prevent access and tampering of medical equipment. Their main security concern was legacy medical equipment that is vital to patient care but cannot be patched or otherwise secured. Harmony IoT provided a lightweight, non-invasive solution that was rapidly deployed in the company's multiple clinics, immediately protecting critical equipment from over-the-air attacks.

ANATOMY OF A WIRELESS ATTACK



With Harmony IoT: Detects rogue AP within seconds, identifies its location, sends alert, prevents any connections to that AP.